

# **GOV'T EXHIBIT 6**

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,  
  
Plaintiff,  
  
v.  
  
KRISHNA VIRAMONTES,  
  
Defendant.

Case No. [16-cr-00508-EMC-1](#)

**ORDER DENYING DEFENDANT'S  
MOTION TO SUPPRESS EVIDENCE**

Docket No. 33

**I. INTRODUCTION**

Defendant Krishna Viramontes has been charged with various child-pornography-related counts as a result of Dropbox's search of his files. Before this Court is Mr. Viramontes' Motion to Suppress Evidence. Docket No. 33 ("Mot.").

**II. PROCEDURAL BACKGROUND**

Mr. Viramontes filed his Motion to Suppress on June 8, 2017, arguing that Dropbox, the National Center for Missing and Exploited Children ("NCMEC"), and Sergeant William Hepler violated his Fourth Amendment rights by conducting various searches of his Dropbox files. Mot. at 10.

Thereafter, the parties filed an Opposition and Reply. The Government's Opposition, Docket No. 36 ("Opp."), included as Exhibit B Dropbox's first declaration via its Content Safety Lead Chengos Lim ("Orig. Decl."). The Court then held an initial hearing on July 26, 2017, and continued the matter to allow for further briefing. After the hearing, the Court issued an order for supplemental briefing, inquiring as to: (1) the degree of public availability of Mr. Viramontes' files, (2) whether Dropbox had established a pattern of search activity and government reporting with regard to child pornography files, and (3) Dropbox's public or private motive in manually

reviewing files. Docket No. 42. After the Government filed an additional declaration from Dropbox via Lim, Docket No. 47, Ex. A (“First Supp. Decl.”), with accompanying arguments, Docket No. 47, (“Gov. First Supp. Brief”), the Court ordered another declaration on the frequency of Dropbox’s NCMEC reporting. Docket No. 51. The Government provided such a declaration from Dropbox via Lim. Docket No. 54 (“Sec. Supp. Decl.”). Mr. Viramontes then submitted a response, Docket No. 57 (“Def. Supp. Reply”), as did the Government. Docket No. 60 (“Gov. Sec. Supp. Brief”). The Court then conducted a second hearing and took the matter under submission.

### III. FACTUAL BACKGROUND

On May 24, 2016, Dropbox submitted a CyberTipline report to NCMEC. *See* Mot., Ex. A (“CyberTipline Report”), at KV 00056. NCMEC is a non-profit organization statutorily charged with acting as a national clearinghouse for reports of child pornography. *See* Opp., Ex. C (“NCMEC Decl.”) ¶ 2; 34 U.S.C. § 11293(b) (detailing NCMEC’s responsibilities); 18 U.S.C. § 2258A(c), (d)(6) (same). When electronic service providers like Dropbox discover child pornography on their services, they are statutorily required to submit a report to NCMEC’s “CyberTipline.” *See* 18 U.S.C. § 2258A(a). After receiving a CyberTipline report, NCMEC conducts an initial investigation. NCMEC Decl. ¶¶ 12-17. It then supplements the CyberTipline report with the results of its investigation and sends the report to law enforcement agencies for further action if appropriate. *Id.* ¶ 20.

Here, Dropbox discovered 10 videos of child pornography on Mr. Viramontes’ Dropbox account. First Supp. Decl. ¶ 16. In accordance with statutory law, it submitted a CyberTipline report regarding those videos. Orig. Decl. ¶ 9. When NCMEC received the report, it conducted its initial investigation, then turned the information over to the San Jose Police Department. NCMEC Decl. ¶¶ 25-27. The instant prosecution ensued.

Dropbox discovered the 10 videos on Mr. Viramontes’ account using [REDACTED]

[REDACTED]. First Supp. Decl. ¶ 16. [REDACTED]

[REDACTED]. *See id.* [REDACTED]

1 [REDACTED]. *Id.* In doing so, Dropbox discovered 10 files in Mr. Viramontes’  
2 Dropbox account that corresponded to child pornography. *See id.*

3 Upon discovering the 10 files on Mr. Viramontes’ account, Dropbox manually opened  
4 each file to confirm that they were child pornography. First Supp. Decl. ¶ 6. It then filed the  
5 CyberTipline report, attaching the 10 apparent child pornography files and 7 additional “log files.”  
6 *Id.* The log files appear to contain meta data on the 10 pornography files, such as upload dates and  
7 file titles. *See* Mot., Ex. B (“SFPD Chronology”), at KV 00153. For each of the 17 files, Dropbox  
8 answered “Yes” to “Was File Reviewed by Company” and “Was File Publicly Available?”  
9 CyberTipline Report, at KV 00060-63.

10 When NCMEC received the CyberTipline report, NCMEC staff opened 8 of the 10  
11 pornography files and searched publicly available records and websites using information from the  
12 report, *e.g.*, the email and IP addresses associated with the Dropbox account. NCMEC Decl.  
13 ¶¶ 24-26; *see also* CyberTipline Report, at KV 00058-60. These searches suggested that the  
14 Dropbox user resided near the San Francisco Bay Area or Sacramento. NCMEC Decl. ¶ 26.  
15 Based on this information, NCMEC forwarded the report and their research to the San Jose Police  
16 Department. *Id.* ¶ 27. The San Jose Police Department’s Internet Crimes Against Children Unit  
17 forwarded the materials to its San Francisco counterpart, where Sergeant Heppler was assigned to  
18 the case. Heppler Decl. ¶ 5. When Sergeant Heppler received the materials, he reviewed the 10  
19 files of child pornography and began his investigation. SFPD Chronology, at KV 00152. This  
20 investigation resulted in Mr. Viramontes’ arrest and prosecution.

#### 21 **IV. DROPBOX’S SEARCHES**

##### 22 **A. Dropbox as Government Agent**

23 Mr. Viramontes argues that Dropbox acted as a government agent when it warrantlessly  
24 conducted [REDACTED] and manually reviewed Mr. Viramontes’ files, thereby violating the  
25 Fourth Amendment. This contention is governed by *United States v. Cleaveland*, under which a  
26 private party’s search is a government action for the purposes of the Fourth Amendment if (1) “the  
27 government knew of and acquiesced in the intrusive conduct,” and (2) “the party performing the  
28 search intended to assist law enforcement efforts.” 38 F.3d 1092, 1093 (9th Cir. 1994), *as*

1 *amended* (Jan. 12, 1995). The defendant bears the burden of proving the *Cleaveland* prongs are  
 2 met. *Id.* With regard to the first prong, knowledge of and acquiescence to a pattern of searching  
 3 (as opposed to the specific search) may suffice. *See United States v. Walther*, 652 F.2d 788, 793  
 4 (9th Cir. 1981). Here, Dropbox has conducted two types of searches—searches [REDACTED]  
 5 and manual reviews of identified files. Each type of search triggers its own *Cleaveland* analysis.

6 1. Government Knowledge of and Acquiescence to Private Search

7 In the instant case, there is no indication that the government knew of or acquiesced to the  
 8 particular Dropbox searches that revealed Mr. Viramontes' files. The question is whether the  
 9 government knew of and acquiesced to "a particular pattern of search activity" that includes the  
 10 disputed search. *Walther*, 652 F.2d at 791-93.

11 Mr. Viramontes argues that the government did because Dropbox has filed many reports  
 12 with the NCMEC in the last several years—in fact, Dropbox reported [REDACTED] illegal images  
 13 in one year alone. *See* Def. Supp. Reply at 7. He also argues that NCMEC's creation of the  
 14 CyberTipline was meant "to assist internet companies like Dropbox in reporting" child  
 15 pornography. *Id.* Finally, Mr. Viramontes cites news reports and a Department of Justice news  
 16 release concerning various child pornography prosecutions involving Dropbox. Reply at 7-8.

17 a. [REDACTED]

18 As to Dropbox's [REDACTED], Mr. Viramontes' evidence establishes government  
 19 knowledge that Dropbox reported child pornography. It does not necessarily establish knowledge  
 20 that Dropbox [REDACTED] or that the government acquiesced to such searching.  
 21 Dropbox has reported many child pornography files to NCMEC, but it learns of such files from  
 22 many sources in addition to [REDACTED]. For example, Dropbox receives reports of child  
 23 pornography from users, Orig. Decl. ¶¶ 5, 7, who might be unwilling solicitees or recipients of  
 24 such files. Dropbox also receives reports of child pornography from law enforcement and  
 25 NCMEC. Orig. Decl. ¶¶ 5, 7. Other evidence cited by Mr. Viramontes is not particularly  
 26 probative. For example, NCMEC's creation of the CyberTipline goes to reporting, not necessarily  
 27 searching. Of the news articles that Mr. Viramontes cites, two indicate only that Dropbox  
 28 provided a tip to NCMEC about child pornography on Dropbox, but does not indicate how

Dropbox obtained the information. *See id.* The other three articles do not indicate that Dropbox took any action at all. *See id.*

While there is no direct evidence of the government's awareness of and acquiescence in Dropbox's [REDACTED], the sheer number of images reported by Dropbox to NCMEC raises an inference of such. Moreover, the general availability of [REDACTED]

[REDACTED].  
*See* Kate Knibbs, *Dropbox Refuses to Explain Its Mysterious Child Porn Detection Software*, Gizmodo (Aug. 12, 2015, 2:36 p.m.), <https://gizmodo.com/dropbox-refuses-to-explain-its-mysterious-child-porn-de-1722573363> ("Dropbox has already admitted to using a hashing system to detect illegal content in its users['] files, but not for child porn—for detecting copyrighted files."). Although it has not disclosed whether and how it searches user files for child pornography, press reports have assumed Dropbox employs such tools, given their availability. *See id.* (speculating that Dropbox uses PhotoDNA, a hash tool, to locate child pornography); Nate Anderson, *After Dropbox Finds a Child Porn Collector, a Chess Club Stops His Knife Attack*, Ars Technica (Nov. 23, 2015, 7:00 a.m.), <https://arstechnica.com/tech-policy/2015/11/how-dropbox-found-a-child-porn-collector-and-a-chess-club-stopped-his-rampage> (Dropbox "has for some time been the target of speculation that it proactively scans user uploads against a database of known illegal imagery."). Although a close question, there is sufficient evidence from which it may be inferred that the government likely knew of and acquiesced in Dropbox's [REDACTED]. *Cf. United States v. Reed*, 15 F.3d 928, 932 n.4 (9th Cir. 1994) (Accepting the fruits of a known pattern of search constitutes acquiescence to that pattern.).

b. Manual Review

As to Dropbox's manual review, Dropbox engaged in a pattern of search. Dropbox reported many files of suspected child pornography from at least May 2016 to August 2017, *see* Sec. Supp. Decl. ¶ 2, and "[a]ll apparent child pornography is manually reviewed by a member of the content safety team before it is reported to NCMEC." Orgi. Decl. ¶ 2; *see also* First Supp. Decl. ¶ 13. The issue then is whether the government knew of and acquiesced in Dropbox's pattern of manually reviewing files containing suspected child pornography before reporting them

1 to NCMEC.

2 The most plausible method by which the government might become aware of Dropbox's  
3 pattern of manual review is via Dropbox's answers to CyberTipline queries. When an electronic  
4 service provider (ESP) files a report with NCMEC, it may answer "Was File Reviewed by the  
5 Company?" NCMEC Decl. ¶ 10. This field is optional. *Id.* When NCMEC receives a report, it  
6 performs an investigation. It then forwards the results of its investigation and the ESP's original  
7 report to law enforcement. *Id.* ¶ 18. Therefore, if an ESP always manually reviews the file and  
8 always chooses to answer "Was File Reviewed by the Company?" in the affirmative, then the  
9 government would know of that ESP's pattern of manual review. In this case, Dropbox always  
10 manually reviews reported files, but the record does not indicate how often it chooses to answer  
11 the "File Reviewed" query. The record reflects only that Dropbox chose to answer in the  
12 affirmative in its NCMEC report regarding Mr. Viramontes' files. *See* CyberTipline Report, at  
13 KV 00060-63. There is no evidence in the record that Dropbox always or often gave the same  
14 affirmative answer in other NCMEC reports. Thus, there is no evidence from which it may  
15 reasonably be inferred that the government was aware of and acquiesced in Dropbox's pattern of  
16 conducting manual review of reported images.

17 The facts in the record herein contrast with *Walther*. In *Walther*, Hank Rivard, an airline  
18 employee, had opened a suspicious overnight case, discovered a white powder inside, and  
19 contacted DEA agents. *Id.* at 790. Rivard had previously opened cases, and the DEA had never  
20 discouraged him from doing so. *Id.* In addition, Rivard had previously been a paid confidential  
21 informant for the DEA for four years. *Id.* The trial court had found that Rivard's sole reason for  
22 opening the case was his suspicion that it contained drugs. *Id.* at 791. It further found that Rivard  
23 "probably opened the case with the expectation that he would be compensated by the DEA if he  
24 were to discover a significant quantity of illegal drugs." *Id.* On appeal, the court held that  
25 Rivard's "prior experience with the DEA provides proof of the government's acquiescence in the  
26 search." *Id.* at 793. Specifically, the DEA "had certainly encouraged Rivard to engage in this  
27 type of search. Rivard had been rewarded for providing drug-related information in the past. He  
28 had opened Speed Paks before, and did so with no discouragement from the DEA. The DEA thus

1 had knowledge of a particular pattern of search activity . . . and had acquiesced in such activity.”  
2 *Id.* at 793. The court “emphasize[d] the narrowness of [this] holding,” specifying that “[i]t is  
3 dependent upon the trial court’s finding of extensive contact between Rivard and the DEA.” *Id.*

4 In the instant case, there is no evidence of the government’s knowledge of prior manual  
5 reviews by Dropbox. Moreover, Dropbox has not been rewarded for these searches, nor is there  
6 any evidence of positive encouragement by the government. Mr. Viramontes therefore has not  
7 shown that the government knew of and acquiesced in Dropbox’s pattern of conducting manual  
8 reviews of suspected child pornography.

9 2. Private Entity’s Intent to Assist Law Enforcement

10 Mr. Viramontes fails to meet his burden under the second prong of *Cleaveland* as to both  
11 the [REDACTED] and manual review. Under that prong, the court examines “whether the  
12 party performing the search intended to assist law enforcement efforts or further his own ends.”  
13 *Cleaveland*, 38 F.3d at 1093. An interest solely in crime prevention is not an independent private  
14 motive. *Reed*, 15 F.3d at 932. Where the private party is motivated by a law enforcement purpose  
15 but also has a “legitimate, independent motivation to further its own ends,” no government  
16 conduct will be found unless the defendant proves that “the level of government involvement” was  
17 “so extensive as to trigger Fourth Amendment scrutiny.” *Cleaveland*, 38 F.3d at 1094 (internal  
18 quotation marks omitted) (citing *Corngold v. United States*, 367 F.2d 1, 5-6 (9th Cir. 1966)). In  
19 this regard, a government agent must “be involved either directly as a participant—not a mere  
20 witness—or indirectly as an encourager of the private person’s search.” *United States v. Leffall*,  
21 82 F.3d 343, 347 (9th Cir. 1996). Contrary to Mr. Viramontes argument, the fact that a private  
22 party intended to further a law enforcement purpose “in some way” does not convert the party’s  
23 conduct into governmental action. *See Reply* at 8-9 (citing *United States v. Ackerman*, 831 F.3d  
24 1292 (10th Cir. 2016)). Under *Cleaveland*, so long as the party had a legitimate, independent  
25 motivation, that motivation “was not negated by any dual motive to detect or prevent crime or  
26 assist the police.” 38 F.3d at 1094.

27 a. [REDACTED]

28 There is no evidence that Dropbox conducted voluntary searches for child pornography



1 with the intent directly to assist law enforcement. In contrast with *Walther*, where “Rivard opened  
2 the case with the expectation of probable reward from the DEA,” 651 F.2d at 792, there is no  
3 indication that Dropbox expected a quid pro quo for its voluntary searches. Though Dropbox is  
4 required by statute to report child pornography, it is not required to search for it. If anything,  
5 Dropbox risked potential liability under 18 U.S. C. § 2258B(c) by searching for child  
6 pornography.

7 To be sure, Dropbox acknowledges it had an interest in searching for child pornography  
8 that may be deemed law-enforcement related. *See* Orig. Decl. ¶¶ 3-4 (describing business interest  
9 in enforcing policies that prohibit illegal content); *Reed* 15 F.3d at 932. However, that interest  
10 was in addition to its legitimate, independent purpose. Specifically, Dropbox conducted voluntary  
11 searches for child pornography, in part because “we do not want our services to be associated with  
12 or used to store [child abuse] content, and . . . users may stop using our services if they encounter  
13 it.” Orig. Decl. ¶ 4. This is a business interest independent of law enforcement.

14 In response, Mr. Viramontes tries to impugn Dropbox’s declarations that asserted such  
15 business interest. He argues that, contrary to Dropbox’s declarations, Dropbox did not search [REDACTED]  
16 [REDACTED] for child pornography in furtherance of a legitimate, independent motivation.  
17 According to Mr. Viramontes, the [REDACTED] threaten Dropbox’s public image as a privacy-  
18 conscious service and therefore run against Dropbox’s business interests. *See* Def. Supp. Reply at  
19 7-8. Since conducting [REDACTED] runs against Dropbox’s business interests, Dropbox could not  
20 have been motivated by those interests when it conducted the [REDACTED], and Dropbox’s  
21 declarations otherwise are “not candid.” *See id.* Instead, Mr. Viramontes asserts Dropbox’s true  
22 interest in conducting [REDACTED] is to assist law enforcement. *See id.* at 10. He also argues  
23 that if Dropbox were truly concerned about removing child pornography from its service, it would  
24 have used the government’s [REDACTED] to identify illicit files. *Id.* at 10.  
25 Instead, Dropbox [REDACTED].

26 Neither of Mr. Viramontes’ arguments is persuasive. It may be that Dropbox’s [REDACTED]  
27 [REDACTED] threaten Dropbox’s privacy-friendly theme and therefore may impair its business  
28 interests. However, it is also plausible that “users may stop using [Dropbox] if they encounter”

child pornography on the service, Orig. Decl. ¶ 4, in which case the [REDACTED] further  
Dropbox's business interests.

Mr. Viramontes' argument regarding Dropbox's decision to [REDACTED] is  
also unconvincing. It may be that using the government's [REDACTED] would have permitted  
Dropbox to more efficiently identify child pornography. However, there is no requirement that  
Dropbox use the best methods available to it. Moreover, Dropbox's decision not to [REDACTED]  
[REDACTED] cuts both ways. Dropbox's [REDACTED] would appear to  
undercut not only its private motive of finding and purging child pornography from its servers, but  
equally its supposed law-enforcement motive. Hence, Dropbox's decision to [REDACTED]  
[REDACTED] is not probative on this issue.

Furthermore, Mr. Viramontes has failed to prove "[a] government agent [was] involved  
either directly as a participant—not a mere witness—or indirectly as an encourager of the private  
person's search." *Leffall*, 82 F.3d at 347. He has not shown that government involvement in  
Dropbox's searches was "so extensive as to trigger Fourth Amendment scrutiny." *Cleaveland*, 38  
F.3d at 1094. Mr. Viramontes has not argued or demonstrated that the government was involved  
in the [REDACTED] in any way. As noted above, there is no reward for searching for child  
pornography, nor is there a statutory command to do so. There is only a requirement to report  
discovered child pornography.

Because Dropbox had a legitimate, independent motive for conducting its [REDACTED],  
and because there was apparently no government involvement in these searches, Mr. Viramontes  
failed to meet the second prong of *Cleaveland* as to the [REDACTED].

b. Manual Review

As to the manual review, Dropbox states that "the primary reason" it conducts such  
reviews is "to protect[] the privacy of its users" whose contents Dropbox would be disclosing to  
NCMEC. First Supp. Decl. ¶ 14. The manual review ensures that only reportable content is  
disclosed to NCMEC. *Id.* Additionally, "[b]ecause manual review is required for potential  
violations reported by individuals, the most consistent and efficient process is to conduct manual  
review for all" such content. *Id.* ¶ 15. Finally, Dropbox cites the [REDACTED]

1 [REDACTED] in identifying child pornography as cause to double check files  
2 identified by [REDACTED]. *Id.* ¶¶ 16-18.

3 In response to these facially legitimate, independent motives, Mr. Viramontes notes that  
4 Dropbox [REDACTED]. Def. Supp. Reply at  
5 4-5. As a result, every file [REDACTED]  
6 [REDACTED] was known to Dropbox to be child pornography; no manual review was necessary. *Id.*  
7 Mr. Viramontes also argues that manual review “runs afoul” 18 U.S.C. § 2258B(c), which requires  
8 companies like Dropbox to minimize the number of employees exposed to child pornography. *Id.*  
9 at 5. Given these reasons not to conduct manual reviews, Mr. Viramontes concludes that  
10 Dropbox’s motive in manually reviewing files must be to destroy its users’ Fourth Amendment  
11 protection therein, permitting the government to open the file without a warrant. *Id.*

12 Mr. Viramontes’ arguments are unconvincing. First, Mr. Viramontes argues that [REDACTED]  
13 [REDACTED]  
14 [REDACTED]  
15 [REDACTED]. First Supp. Decl. ¶¶ 17-18. Dropbox also states that [REDACTED]  
16 [REDACTED]. *Id.* Confronted with [REDACTED]  
17 [REDACTED], Dropbox implemented the manual search to confirm that identified files are child  
18 pornography before submitting a CyberTipline report. *Id.* As to the risk of liability under  
19 § 2258B(c), a company might plausibly undertake such risk for business purposes, such as to  
20 ensure only child pornography is reported and thereby avoid wrongfully jeopardizing its users’  
21 reputations. Mr. Viramontes fails to discredit Dropbox’s stated purposes in manually reviewing  
22 possible child pornography.

23 Because Dropbox had a legitimate private motive in conducting manual reviews, Mr.  
24 Viramontes must show that government involvement in these reviews was “so extensive as to  
25 trigger Fourth Amendment scrutiny.” *Cleaveland*, 38 F.3d at 1094. Again, Mr. Viramontes has  
26 not demonstrated that the government was involved in or encouraged the manual review in any  
27 way. *See Leffall*, 82 F.3d at 347; *cf. Walther*, 652 F.2d at 793 (finding that airline employee was  
28 government agent was dependent on extensive government involvement, including prior rewards

and encouragement).

For the foregoing reasons, Mr. Viramontes failed to meet his burden under the second prong of *Cleaveland* as to the manual reviews.

c. Conclusion

Mr. Viramontes has not proved under *Cleaveland* that Dropbox acted as a government agent when it conducted [REDACTED] and manual review of Mr. Viramontes' files.

B. Consent

There is a second reason to deny Mr. Viramontes' motion to suppress. The evidence shows he consented to Dropbox's search of his files. "The standard for measuring the scope of a suspect's consent under the Fourth Amendment is that of 'objective' reasonableness—what would the typical reasonable person have understood by the exchange [granting consent]?" *Florida v. Jimeno*, 500 U.S. 248, 251 (1991).<sup>1</sup>

When Mr. Viramontes created and used his Dropbox account, he agreed to Dropbox's Terms of Service. *See* Orig. Decl., Ex. A. The Terms unequivocally permit Dropbox to "review your conduct and content for compliance with these Terms and our Acceptable Use Policy." *Id.* at ECF 6. The Acceptable Use Policy clearly prohibits users from using the service to "publish or share materials that are unlawfully pornographic or indecent" or to "violate the law in any way." *Id.* at ECF 11. Mr. Viramontes does not deny that he was aware of and agreed to the Terms of Service or Acceptable Use Policy. Instead, he contests only the specificity of the consent, arguing that "[n]othing in Dropbox's terms of use indicates that it searches private user accounts for illegal content." Reply at 12. He argues the Terms of Service and Acceptable Use Policy do not contain the specific words "search" and "monitor." *Id.* As a result, he argues, he could not have

<sup>1</sup> *United States v. Shaibu* appears to require that consent to a search be "intelligently given." 920 F.2d 1423, 1426 (9th Cir. 1990). Given the terms of service, that standard was met here. In any event, that higher standard in *Shaibu* appears to have been based on the special status of the home in Fourth Amendment jurisprudence and is not applicable here. *See id.* The Court also notes that the Second Circuit has criticized *Shaibu* as inconsistent with *Schneckloth v. Bustamonte*, 412 U.S. 218, 235-46 (1973), which held that consent to a search need not be knowing and intelligent. *See United States v. Garcia*, 56 F.3d 418, 424 (2d Cir. 1995) (noting inconsistency); *see also Blakewood v. Harley*, No. C 11-0142 LHK (PR), 2014 WL 877708, at \*4 n.2 (N.D. Cal. Mar. 3, 2014) (same and citing *Garcia*).

“anticipat[ed] the breadth and depth of Dropbox’s intrusions.” *Id.* at 13.

However, a “typical reasonable person,” *Jimeno*, 500 U.S. at 251, would have understood these terms to permit Dropbox to search its users’ files for unlawful content. The prohibition on sharing unlawful pornography together with permitting Dropbox to review “your conduct and content for compliance” could hardly mean anything other than a warning to users that Dropbox could search their files for unlawful pornography. *Cf. Jimeno*, 500 U.S. at 249, 251 (as the officer’s stated intent was to search for drugs, it was reasonable for the officer to conclude that the defendant’s consent extended to containers in the car that might bear drugs).

### C. Reasonable Expectation of Privacy

There is a third reason to deny Mr. Viramontes’ motion to suppress. In order to prevail on his Motion to Suppress, Mr. Viramontes must show that the government either intruded on his reasonable expectation of privacy (“REP”) or committed a common law trespass upon his person, houses, papers, or effects. *United States v. Jones*, 565 U.S. 400, 409 (2012). As Mr. Viramontes’ physical property interests have not been invaded, *see* Part V, *infra*, Mr. Viramontes must show that he had a reasonable expectation of privacy in his files.

Under the reasonable expectation of privacy test, the defendant “must have both a subjective and an objectively reasonable expectation of privacy.” *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). A defendant has a subjective expectation of privacy where he “manifest[s] a subjective expectation of privacy in the object of the challenged search,” and that expectation is objectively reasonable where “society is willing to recognize that expectation as reasonable.” *California v. Ciraolo*, 476 U.S. 207, 211 (1986) (citing *Smith v. Maryland*, 442 U.S. 735, 740 (1979)). Where a defendant exposes the disputed information to the public, however, his REP in that information is destroyed. *Katz*, 389 U.S. at 351.

Each Dropbox file has a privacy setting with three options from which the user may choose: (1) keep the file private (inaccessible to anyone other than the user), (2) share the file with specific Dropbox users, who may then access the file by logging into their Dropbox account, and (3) create a URL for the file. First Supp. Decl. ¶¶ 2-7. When a user selects the URL option, Dropbox creates a URL for the file, whereupon the user can send the URL to others and anyone

1 with the URL can access the file. *Id.* Mr. Viramontes chose the third option, creating URLs for  
 2 each of the 10 files at issue. Orig. Decl. ¶ 10; First Supp. Decl. ¶ 6. Mr. Viramontes does not  
 3 dispute that he did so; he asserts only that he is “almost certain” that he never sent the URLs to  
 4 anyone. Docket No. 46 ¶¶ 3-4; *see also* Def. Supp. Reply at 5.<sup>2</sup>

5 As an extra wrinkle, Dropbox employs a technical measure called a “<META> tag” to  
 6 request that search engines not index its users’ publicly available files. First Supp. Decl. ¶ 5.  
 7 Because of this, Mr. Viramontes’ 10 files would not have been locatable using popular search  
 8 engines. This, however, does not bolster Mr. Viramontes’ subjective expectation of privacy,  
 9 because there is no indication that he knew of or relied on this measure.

10 The facts before the Court establish that Mr. Viramontes uploaded the 10 files to Dropbox,  
 11 and then opted for the least private setting for each of them by creating publicly accessible URLs  
 12 to the files. If Mr. Viramontes had wanted to share his files privately, he could have done so using  
 13 the second, intermediate privacy setting, which would not have allowed broad public access to his  
 14 files. If Mr. Viramontes had not wanted to share his files, he could have opted for the first, most  
 15 private setting. Given that Mr. Viramontes passed over two protective privacy settings in favor of  
 16 a setting that permitted public access to his files, he did not manifest an expectation of privacy.

17 Though not necessary to this order, the Court notes that Mr. Viramontes also would fail the  
 18 objective prong of the *Katz* test. Mr. Viramontes’ 10 files were accessible to the public due to the  
 19 URL privacy setting, although they were difficult to locate due to the <META> tag which made  
 20 conventional Internet search tools ineffective. The situations is somewhat analogous to that in the  
 21 unpublished Ninth Circuit memorandum decision *United States v. Andrews*, 923 F.2d 863, 1991  
 22 WL 3070 (9th Cir. 1991) (unpublished memorandum decision). In that case, Andrews had  
 23 traveled to a publicly accessible, “rugged, remote area” to conduct illegal activities not specified in  
 24

---

25 <sup>2</sup> Though Mr. Viramontes asserts that he did not allow “public access” to his Dropbox files and  
 26 that his files were not “available to the general public,” Docket No. 46, he meant this only in the  
 27 sense that a member of the public would need the URL to access the file. Docket No. 45 at 3:10-  
 28 13 (“[T]he general public . . . could not have accessed the folders at issue here unless . . . of the  
 general public somehow guessed . . . the url of the folder(s).”). Mr. Viramontes does not argue  
 that he did not select the URL option. Dropbox’s declarations that he selected the URL option are  
 credible and not disputed.

the opinion. *Id.* at \*1. Law enforcement officers, acting on tips, followed Andrews and surveilled him using binoculars, a telescope, and a camera. *Id.* This ultimately led to Andrews' conviction. On appeal, Andrews argued that the officers' actions violated his REP. The Ninth Circuit disagreed: "Here, all the observations involved activities or objects in plain view. Anyone can enter the federally-owned lands in question. That Andrews took steps to go to a remote area of public land to hide his criminal activity does not make his expectation of privacy reasonable under the fourth amendment." *Id.* Andrews suggests that Mr. Viramontes' files were without Fourth Amendment protection because they were publicly available, and the fact that they were hard to locate is immaterial.

#### V. NCMEC'S AND SERGEANT HEPPLER'S SEARCHES

Mr. Viramontes argues that NCMEC and Sergeant Heppler also violated the Fourth Amendment when they conducted their respective searches on the 10 video files attached to the CyberTipline report. Mot. at 10, 13-14. Upon receipt of the report and without a warrant, NCMEC staff had viewed 8 of the 10 child pornography files, *see* NCMEC Decl. ¶ 24, and Sergeant Heppler had opened all 10 of the files. SFPD Chronology, at KV 00152.

##### A. Reasonable Expectation of Privacy and Common Law Trespass

Mr. Viramontes argues that NCMEC's actions are subject to the Fourth Amendment because it is a government entity or agent. Mot. at 8. The basis for his argument is that NCMEC is charged by statute to aid law enforcement efforts in various ways pertaining to missing and exploited children, including operating the CyberTipline. *Id.* (citing 18 U.S.C. § 2258A and 42 U.S.C. § 5773, now at 34 U.S.C. § 11293). The government responds that NCMEC is not a government entity or agent and that, in any case, NCMEC merely replicated Dropbox's search. Opp. at 16-18. The government prevails under its latter argument, and the Court therefore need not decide whether NCMEC is a government entity or agent.

"The Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated." *United States v. Jacobsen*, 466 U.S. 109, 117 (1984). Where a private party has performed a search, "the legality of the governmental search must be tested by the scope of the antecedent private search." *Id.* at 115.



Here, Dropbox had opened each of the 10 video files to confirm that they contained apparent child pornography, eviscerating Mr. Viramontes' expectation of privacy in those files. NCMEC then opened 8 of the files. Because NCMEC did not exceed the scope of Dropbox's search, even if it were a government agent, it did not violate the Fourth Amendment.

Mr. Viramontes argues that even if he could not prevail under *Katz*'s reasonable expectation of privacy standard, he prevails under *United States v. Jones*, 565 U.S. 400 (2012). In *Jones*, the Supreme Court held that "the *Katz* reasonable-expectation-of-privacy test has been added to, not substituted for, the common-law trespassory test." *Id.* at 409 (emphasis original). Mr. Viramontes argues that NCMEC trespassed on Mr. Viramontes' Dropbox account when it "seized and searched the files in Dropbox's cybertip," thereby violating the Fourth Amendment. Reply at 16.

*Jones*, being rooted in physical trespass, is inapplicable. In *Jones*, "[t]he Government physically occupied private property for the purpose of obtaining information." 565 U.S. at 404. This implicated the Fourth Amendment, because "such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted." *Id.*; see also *id.* at 407-11 (describing cases involving "physical intrusion" and "physical contact"). Though Mr. Viramontes cites *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016), *reh'g denied* (Oct. 4, 2016), which extended *Jones* to the electronic context, this non-binding decision ignores *Jones*' roots in common law trespass and is unpersuasive. Other courts have declined to apply *Jones* in similar cases. See, e.g., *United States v. Lien*, No. 16-cr-00393-RS-1, Docket No. 45 at 7-8 (N.D. Cal. May 10, 2017), available at Opp., Ex. A, Attach. B (NCMEC did not trespass on defendant's property within meaning of *Jones* when it opened files reported by Google, and *Ackerman*'s holding to the contrary is "simply unpersuasive.").<sup>3</sup>

<sup>3</sup> The Court notes that whether there is a Fourth Amendment violation based on *Jones*' trespass theory is a different inquiry from whether, e.g., a statute enacted by Congress concerning computer hacking may be based upon or borrows concepts from common law trespass. Cf. Computer Fraud and Abuse Act, 18 U.S.C. § 1030; *hiQ Labs, Inc. v. LinkedIn Corp.*, \_\_\_ F. Supp. 3d. \_\_\_, 2017 WL 3473663 (N.D. Cal. Aug. 14, 2017). The Fourth Amendment inquiry appears to examine trespass standards at the time of the Fourth Amendment's adoption. See *Jones*, 565 U.S. at 404-05, 406.



No party has physically trespassed upon Mr. Viramontes' property. Where such "a classic trespassory search is not involved . . . resort must be had to *Katz* analysis." *Id.* at 412-13. In particular, "[s]ituations involving merely the transmission of electronic signals without trespass would remain subject to *Katz*." *Id.* at 411 (emphasis omitted). Such is the case here, and as discussed above, Mr. Viramontes cannot prevail under *Katz*. NCMEC did not violate Mr. Viramontes' Fourth Amendment rights.

Mr. Viramontes' argument regarding Sergeant Heppler's search of the files reported in the CyberTipline also relies on a *Jones* trespass. *See* Mot. at 13-14. For the reasons stated above, *Jones* is inapplicable. Furthermore, because Sergeant Heppler remained within the scope of Dropbox's search by opening the 10 reported child pornography files, he did not intrude upon Mr. Viramontes' reasonable expectation of privacy. Sergeant Heppler therefore did not violate Mr. Viramontes' Fourth Amendment rights.

B. Good-Faith Exception

In addition to the above, there is a further reason to deny Mr. Viramontes' motion to suppress: the good faith exception to the exclusionary rule. Under the good-faith exception, evidence obtained through a wrongful search may be excluded where "a reasonably well trained officer would have known that the search was illegal in light of all of the circumstances." *Herring v. United States*, 555 U.S. 135, 145 (2009) (quoting *United States v. Leon*, 468 U.S. 897, 922 n.23 (1984) (internal quotation marks omitted)). "[P]olice conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Id.* at 144. "But when the police act with an objectively reasonable good-faith belief that their conduct is lawful, or when their conduct involves only simple, isolated negligence," exclusion is not appropriate. *Id.* at 238.

Here, the good-faith exception precludes exclusion even if Dropbox had not manually reviewed the files searched by NCMEC and Sergeant Heppler, and even if Dropbox were a government agent.

1. Good-Faith Exception Where Dropbox Did Not Manually Review the Files

Even if Dropbox had not manually reviewed the 10 child pornography files, the good-faith

1 exception to the exclusionary rule applies to NCMEC's and Sergeant Heppler's searches.

2 In *Herring*, an officer had arrested and searched the defendant based on an erroneous entry  
3 in an arrest warrant database. *Herring*, 555 U.S. at 137. The Supreme Court held that the good-  
4 faith exception applied to the officer's conduct, because the conduct was insufficiently culpable to  
5 require exclusion. *Id.* at 144. In other words, "the good faith exception was met because the  
6 officer reasonably relied on an external source, which turned out to be erroneous." *United States*  
7 *v. Camous*, 773 F.3d 932, 944 (9th Cir. 2014) (emphasis omitted) (discussing *Herring*). Here,  
8 Dropbox's CyberTipline report prominently indicated that Dropbox had reviewed each child  
9 pornography file. See CyberTipline Report, at KV 00060-63 (answering "Yes" to "Was File  
10 Reviewed by the Company?" for each file). A reasonably well-trained officer considering the  
11 CyberTipline report would have no reason to doubt that Dropbox had already opened the files and  
12 that his own review of the same would implicate no further Fourth Amendment interest.

13 2. Good-Faith Exception Where Dropbox Was a Government Agent

14 Similarly, even if Dropbox were a government agent and the searches by Dropbox violated  
15 the Fourth Amendment, the good-faith exception precludes exclusion of evidence on that basis. In  
16 good-faith inquiries involving multiple government entities, "[i]t is necessary to consider the  
17 objective reasonableness, not only of the officers who eventually executed a warrant, but also of  
18 the officers . . . who provided information material to the probable-cause determination." *United*  
19 *States v. Leon*, 468 U.S. 897, 923 n.24 (1984). An officer cannot obtain a search warrant by  
20 improper means, pass it to an innocent colleague for execution, and expect the good-faith  
21 exception to protect the resulting search. *Id.* Thus, if Dropbox were a government agent, both  
22 Dropbox's and Sergeant Heppler's actions must have been objectively reasonable for the good-  
23 faith exception to apply.

24 Here, Dropbox voluntarily conducted searches with no involvement by law enforcement.  
25 A reasonably well-trained officer, whether in Dropbox's, NCMEC's, or Sergeant Heppler's shoes,  
26 would not have concluded that Dropbox were a government agent. See Part IV.A, *supra*.  
27 Moreover, a reasonably well-trained officer would have concluded that Mr. Viramontes consented  
28 to Dropbox's search in any case. See Part IV.B, *supra*.

Viramontes' argument in response relies on a part of the good-faith exception doctrine stemming from *Davis v. United States*, 564 U.S. 229 (2011). In *Davis*, officers had conducted a search in compliance with then-binding circuit precedent, but while appeal was pending in *Davis*, the Supreme Court held in a separate case that such searches are unconstitutional. Yet when *Davis* reached the Supreme Court, the Court held that exclusion was not warranted, because the officers' actions were insufficiently deliberate and culpable, being in reliance on binding precedent. *Id.* at 240. The Court noted that the officers had not acted "deliberately, recklessly, or with gross negligence," or even "recurring or systemic negligence." *Id.* Therefore, "searches conducted in objectively reasonable reliance on binding appellate precedent are not subject to the exclusionary rule." *Id.* at 231. Mr. Viramontes argues that *Davis* requires binding appellate precedent to trigger the good-faith exception and that such precedent is not present here. Reply at 19. For support, he cites *United States v. Lara*, in which the Ninth Circuit opined in dicta that *Davis* should not be expanded to "cases in which the appellate precedent, rather than being binding, is (at best) unclear." 815 F.3d 605, 613 (9th Cir. 2016).

Mr. Viramontes' reliance on *Lara* is insufficient. Even accepting *Lara*'s dicta regarding the limits of the *Davis* "binding appellate precedent" rule, that rule is only one facet of the good-faith exception. The touchstone of the good-faith exception remains "whether a reasonably well trained officer would have known that the search was illegal . . . . In making this determination, all of the circumstances . . . may be considered." *Leon*, 468 U.S. at 922, n.23. As discussed above, NCMEC, Dropbox, and Sergeant Heppler acted reasonably and without the deliberateness and culpability necessary to trigger exclusion. Dropbox conducted its searches voluntarily without coercion or encouragement by the government; it pursued an independent business interests; and there was no substantial government involvement in the search of Mr. Viramontes' files. Neither NCMEC, Dropbox, nor Sergeant Heppler have any significant reason to believe Dropbox was acting as a government agent, a fact necessary to implicate the Fourth Amendment.

For the foregoing reasons, the good-faith exception precludes suppression of evidence, even if Dropbox had not manually reviewed the 10 apparent child pornography files or if Dropbox were a government agent.

## VI. EVIDENTIARY HEARING

Mr. Viramontes requests an evidentiary hearing so that he can test the credibility of Dropbox's declarations. In particular, Mr. Viramontes points to Dropbox's inaccurate declaration that all 17 files in its CyberTipline report were publicly shared and manually reviewed. Orig. Decl. ¶¶ 10-11. This representation also appears in Dropbox's CyberTipline report. *See* CyberTipline Report KV 00060-63. In its second declaration, Dropbox corrected itself, stating that only the 10 child pornography files were publicly shared and manually reviewed, and that the other 7 files were automatically generated log files (and thus were not publicly available). First Supp. Decl. ¶ 6.

Mr. Viramontes argues that Dropbox's inaccurate original declaration casts doubt on whether Dropbox actually manually reviewed the 10 child pornography files. Def. Supp. Reply at 2-4. Specifically, he argues that if Dropbox employees had manually reviewed all 17 files as claimed in the CyberTipline report, they would have seen that 7 of the files were internal log files and would not have marked them as publicly available. *Id.* at 3-4. The 7 log files were nevertheless marked publicly available in the CyberTipline report. *See* CyberTipline Report, at KV 00060-63. Mr. Viramontes thereby concludes that the log files' "Yes" boxes for "Was File Reviewed by Company?" and "Was File Publicly Available?" were checked automatically and without accompanying manual review—and that the 10 child pornography files' boxes likely were also checked automatically and without manual review. Def. Supp. Reply at 4. In addition, Mr. Viramontes argues that Dropbox's incorrect statement regarding the 7 log files casts doubt on all of Dropbox's declarations generally. *Id.* at 3.

"An evidentiary hearing on a motion to suppress need be held only when the moving papers allege facts with sufficient definiteness, clarity, and specificity to enable the trial court to conclude that contested issues of fact exist." *United States v. Howell*, 231 F.3d 615, 620 (9th Cir. 2000). Where suppression does not turn on the facts at issue, however, an evidentiary hearing is unnecessary. *See id.* at 621.

Here, Dropbox via its Content Safety Lead Chengos Lim stated that all 17 files were publicly shared and manually reviewed. It then corrected itself, stating that only the 10 apparent

child pornography files were publicly shared and manually reviewed. That is all that Mr. Viramontes has pointed to. This contradiction is insufficient to create a disputed fact. First, Mr. Viramontes argues that all of Dropbox's declarations are thrown into doubt because "[i]f Ms. Lim actually reviewed the files at issue here prior to writing her first declaration," she would have known that 7 of the files were log files, not publicly available child pornography files. Def. Supp. Reply at 3. But the original declaration does not state that Lim reviewed the 17 files. It states only that "Dropbox's records reflect that all 17 files" were publicly shared and manually reviewed. Orig. Decl. ¶¶ 10-11. Second, after realizing its mistake, Dropbox reaffirmed that the 10 video files were publicly shared and manually reviewed. First Supp. Decl. ¶ 6. Dropbox's mistake in its original declaration, while creating some uncertainty, does not cast doubt on this subsequent reaffirmation. Third, Dropbox separately stated that, as a matter of operational efficiency, its policy is to manually review all potential child pornography files before submission to NCMEC, regardless of how they are discovered. Orig. Decl. ¶ 8; First Supp. Decl. ¶ 14. The 10 files would have been subject to this policy, and nothing other than the singular overstatement of files reviewed casts doubt on the existence of this policy. Finally, Dropbox voluntarily revealed its mistake. Neither party had noticed the mistake, and Dropbox could have remained silent, in which case the mistake might never have surfaced. That Dropbox noticed and revealed the mistake lends credibility to its subsequent reaffirmation regarding the search of the 10 files.

Though this is sufficient to deny Mr. Viramontes' request for an evidentiary hearing, an evidentiary hearing regarding a motion to suppress may be denied where there are "no facts which, if proved, would allow the court to suppress" the evidence. *Howell*, 231 F.3d at 621. Even if Mr. Viramontes were able to prove that Dropbox had not manually reviewed the 10 video files, the good-faith exception precludes suppression.

///

///

///

///

///


**VII. CONCLUSION**

For the foregoing reasons, the motion to suppress and request for evidentiary hearing are  
**DENIED.**

This order disposes of Docket No. 33.

**IT IS SO ORDERED.**

Dated: November 14, 2017

  
EDWARD M. CHEN  
United States District Judge